Deutscher Bundestag **Drucksache 15/2127**

15. Wahlperiode 03. 12. 2003

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Horst Friedrich (Bayreuth), Ulrike Flach, Birgit Homburger, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 15/2026 –

Datenschutz und Datensicherheit bei der LKW-Maut

Vorbemerkung der Fragesteller

Neben der technisch bedingten Verzögerung bei der Einführung der LKW-Maut, der beihilferechtlichen Problematik des Themas und der generellen Diskussion über die Verwendung der Mautmittel („zusätzlich"), gewinnt in letzter Zeit ein weiteres Thema in der öffentlichen Diskussion über die LKW-Maut an Bedeutung. Es handelt sich um Bedenken auf dem Gebiet des Datenschutzes und der Datensicherheit. Anknüpfungspunkt ist die Tatsache, dass bei Durchfahrten an den Maut-Kontrollbrücken alle Fahrzeuge, LKW und PKW, fotografiert werden. Mit dem Kontrollsystem wird somit der gesamte fließende Verkehr erfasst, wobei die mautpflichtigen LKW aus der Gesamtmenge der Daten herausgefiltert und die Fotos der übrigen Fahrzeuge gelöscht werden sollen. Bei der automatischen Einbuchung durch die so genannten On-Bord-Units (OBU) wird jede Autobahnbenutzung eines LKW per Satellitennavigation mit Positions- und Fahrzeugdaten registriert und über GSM-Mobilfunk an die Betreibergesellschaft übermittelt.

Für besondere Aufmerksamkeit hat die Entscheidung eines Gummersbacher Amtsrichters gesorgt, der verfügt hatte, dass die Betreiberfirma Toll Collect Daten aus dem Probetrieb zur Strafverfolgung nach dem Diebstahl eines Container-LKW herausgeben sollte. Toll Collect hat sich aus Rechtsgründen verweigert, wobei die Herausgabe der Daten – ohne abschließende rechtliche Klärung – offenbar daran gescheitert ist, dass das Erfassungssystem aus den bekannten Gründen noch nicht richtig funktionierte und die Daten deshalb nicht in der notwendigen Weise zur Verfügung standen. Gleichwohl wirft dieser Fall die Frage auf, ob eine solche Verwendung der Maut-Daten zulässig ist oder nicht.

Die Akzeptanz der partei- und verbändeübergreifend als notwendig erachteten LKW-Maut hängt auch davon ab, dass die Nutzer dem System auch in datenschutzrechtlicher Hinsicht vertrauen. Hacker-Angriffe auf die Erfassungsdaten und die Abrechnungskommunikation per Mobiltelefon müssen ausgeschlossen sein. Ausgeschlossen sein muss auch, dass Nicht-Berechtigte das Bewegungsprofil eines LKW ausspionieren können. Deshalb müssen die Vertraulichkeit und Integrität der in der OBU gespeicherten und per GSM übertragenen Daten gesichert sein.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Verkehr, Bau- und Wohnungswesen vom 2. Dezember 2003 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

1. Kann das GPS-Signal in den OBU, die neben einem Mikroprozessor auch einen GPS-Empfänger und ein GSM-Mobiltelefon enthalten, manipuliert werden?

Die in der On-Bord-Unit (OBU) gespeicherten Daten werden mit Hilfe kryptographischer Verfahren vor Manipulationen durch Dritte geschützt. Das Risiko der Manipulation des GPS-Signals – im Sinne einer Veränderung von Positionsdaten über das GPS-Signal – wird aufgrund der lokal begrenzten Wirksamkeit und des hohen technischen Aufwands als gering angesehen.

2. Trifft es zu, dass die von Toll Collect verwendete Technik ermöglicht, ein Bewegungsprofil aller registrierten LKWs herzustellen und damit eine vollständige Überwachung des gesamten Verkehrs möglich ist mit der Folge, dass prinzipiell jedermann (der die dazu notwendige Technik besitzt) die Position eines bestimmten LKW feststellen kann?

Der „gesamte Verkehr“ unterliegt nicht der Mautpflicht. Die Mautpflicht betrifft nur Fahrzeuge des Güterkraftverkehrs mit einem zulässigen Gesamtgewicht ab 12 Tonnen. Es besteht kein Zwang zu Einbau und Nutzung einer OBU. Die vollständige Überwachung des Gesamtverkehrs ist damit schon vom Systemkonzept her nicht möglich.

Innerhalb des LKW-Mautsystems ist darüber hinaus ein umfangreiches Datensicherheitskonzept umgesetzt, das vielfältige Maßnahmen zum Schutz der Daten gegen Manipulation und Missbrauch enthält. Dazu gehören neben grundlegenden organisatorischen Maßnahmen, wie z. B. dem Betrieb von Rechnersystemen ausschließlich in gesicherten Bereichen und entsprechenden Zutrittsrechten nur für autorisiertes Personal, auch komplexe technische Maßnahmen, die die missbräuchliche Verwendung von mautspezifischen Daten durch Dritte verhindern (Verschlüsselungstechniken). Das unbefugte Auslesen der OBU ist somit ausgeschlossen, d. h. dass durch Dritte die Position eines einzelnen LKW nicht ermittelt werden kann.

Die Ortung eines Mobilfunkmodems ist grundsätzlich unter Einsatz entsprechend geeigneter Verfahren möglich, wie sie für den Betrieb eines GSM-Netzes benötigt werden. Es handelt sich dabei jedoch um eine Systemeigenschaft der GSM-Technologie, die für alle Nutzer eines Mobilfunktelefons gilt, nicht nur für die mit einer OBU ausgerüsteten LKW.

3. Können die Daten der OBU, wie Aufenthaltsort oder Geschwindigkeit, durch einen Anruf per Mobilfunk aus den OBU herausgelesen werden?

Das unbefugte Auslesen der OBU wird durch die in der Antwort zu Frage 2 dargestellten Sicherheitsvorkehrungen ausgeschlossen. Die GPS-Koordinaten werden in der OBU nur zur Ermittlung der mautpflichtigen Strecke verarbeitet. Über das GSM-Datenmodem wird verschlüsselt eine errechnete Autobahnabschnitts-ID übermittelt (siehe Antwort zu Frage 1). Mit dem GSM-Modem ist keine Sprachkommunikation möglich.

4. In welcher Weise sind OBU vor dem Herauslösen und vor Manipulation der Daten bei Diebstahl oder Missbrauch der OBU geschützt?

Ein Herauslösen oder Diebstahl der OBU kann nicht restlos ausgeschlossen werden. Im Falle eines Diebstahls kann die OBU durch Toll Collect deaktiviert werden, d. h. sie wird für die Erhebung unbrauchbar.

In der OBU sind Schutzmaßnahmen implementiert, die in jedem Fall eine Manipulation der Daten in der OBU ausschließen. Darüber hinaus wird das unbefugte Auslesen der Daten der OBU durch besondere Sicherheitsverfahren der Verschlüsselung der Schnittstellen und der sicheren Authentisierung verhindert.

5. Sind die per Mobilfunk übertragenen Daten abhörsicher?

Ein unbefugtes Abhören der übertragenen Daten wird aufgrund zusätzlicher kryptographischer Sicherheitsvorkehrungen bei der Nutzung des Mobilfunks ausgeschlossen.

6. Ist nach Auffassung der Bundesregierung sichergestellt, dass durch die gleichzeitige Erfassung der Kennzeichen von nicht-mautpflichtigen Fahrzeugen der Missbrauch für amtliche oder nicht-amtliche erkennungsdienstliche Funktionen ausgeschlossen ist, wie beispielsweise die Überwachung des Standortes, der Fahrtrouten oder der Geschwindigkeiten?

Ein Missbrauch der Daten bei der Erfassung der Kennzeichen von nicht mautpflichtigen Fahrzeugen ist ausgeschlossen. Die Erfassung der Fahrzeuge an den Kontrollbrücken erfolgt gemäß den gesetzlichen Vorgaben. Zunächst werden alle Fahrzeuge erfasst. Es wird ein digitales Übersichtsbild erstellt und eine digitale Frontaufnahme des Kennzeichens. Der Fahrer ist nicht zu erkennen. Bei der Durchfahrt unter der Brücke wird das Fahrzeug vermessen, d. h. Länge, Breite und Höhe und die Achszahl festgestellt.

Soweit feststeht, dass es sich um ein nicht mautpflichtiges Fahrzeug handelt, werden die Vermessungsdaten und die Daten der digitalen Fotos unmittelbar aus dem Speicher der Brücke, dem so genannten Cache, gelöscht. Mit dem oben beschriebenen Verfahren ist eine Feststellung des Standortes bei den nicht mautpflichtigen Fahrzeugen, der Fahrtrouten und der Geschwindigkeit nicht möglich. Die für eine Geschwindigkeitskontrolle zu erfüllenden Anforderungen, wie zum Beispiel eine geeichte Geschwindigkeitsmessung oder die Bildaufnahme des Fahrzeuglenkers, werden durch die Kontrollbrücken nicht erfüllt. Des Weiteren erlaubt das geplante Kontrollnetz mit 300 Kontrollbrücken sowie das Stichprobenverfahren keine Ermittlung von Fahrtrouten und Geschwindigkeitsfeststellungen.

Für die mautpflichtigen Fahrzeuge hat der Gesetzgeber eine eindeutige datenschutzrechtliche Regelung in den §§ 4, 7 und 9 Autobahnmautgesetz für schwere Nutzfahrzeuge (ABMG) getroffen. Nach § 4 Abs. 2 Satz 3 und § 7 Abs. 2 Satz 2 ABMG dürfen die Mauterhebungs- und Mautkontrolldaten ausschließlich zum Zwecke des ABMG verarbeitet und genutzt werden. Eine anderweitige Nutzung ist daher unzulässig.

7. Sind die Kontrollbrücken mit einer Erweiterungsoption für erkennungsdienstliche Funktionen oder Tempokontrollfunktionen ausgerüstet?

   Wenn ja, entspricht dies nach Auffassung der Bundesregierung dem Prinzip der Datensparsamkeit und den Vorgaben der Projektausschreibung, die sich allein auf die Gebührenerfassung von LKW beschränkte?

Die Kontrollbrücken dienen ausschließlich der Ermittlung von Mautprellern. Erweiterungsoptionen über die Kontrolle der Maut hinaus existieren nicht.

8. Sind nach Auffassung der Bundesregierung alle notwendigen Vorkehrungen insbesondere hinsichtlich der Fotografien zum Datenschutz und zur Datensicherheit getroffen?

Ja. Das Kontrollsystem erfüllt das Prinzip der Datensparsamkeit und die Vorgaben der Projektausschreibung hinsichtlich Datenschutz und Datensicherheit. Der Fahrer ist auf dem Foto nicht zu erkennen.

9. Wie beurteilt die Bundesregierung das Risiko, dass in Krisenzeiten das GPS-Signal von den USA ungenau geschaltet oder ganz abgeschaltet wird?

   Wie beurteilt die Bundesregierung die Möglichkeit von Störungen durch unberechtigte Dritte?

Grundsätzlich besteht jederzeit die Möglichkeit, dass der Betreiber des GPS-Systems, das Verteidigungsministerium der USA, das GPS-Signal verschlechtert oder ganz abschaltet. Da dies nach bisheriger Praxis nur in Krisengebieten während des Einsatzes von Militär erfolgt ist, schätzt die Bundesregierung das Risiko für das Gebiet der Bundesrepublik Deutschland derzeit als äußerst gering ein. Die USA haben versichert, ihre Verantwortung gegenüber zivilen und kommerziellen Nutzern ernst zu nehmen.

Um kurzzeitige Unterbrechungen des GPS-Empfangs auszugleichen, ist die OBU mit zusätzlichen Sensoren (Gyro, Tachoabgriff) versehen. Für örtlich bedingte Einschränkungen des GPS-Empfangs ist der Einsatz von Stützbaken vorgesehen.

Technisch ist jedes Funksystem durch Unberechtigte störbar. Da aber jede Störung eines zugelassenen Funksystems strafbewehrt ist und jeder Störsender leicht zu orten ist, sind hier wirksame Möglichkeiten zur Abwehr gegeben.

10. Wie beurteilt die Bundesregierung den Stand der Vorbereitungen des gesamten Maut-Erfassungssystems auf eine spätere Umschaltung vom GPS-Signal auf das viel genauere Galileo-Signal nach Implementierung dieses Systems im Weltraum?

Nach dem derzeitigen Stand der Planungen soll das Galileo-System im Jahre 2008 vollständig in Betrieb sein. Aufgrund der modularen Aufbauweise ist das LKW-Mautsystem prinzipiell in der Lage, nach der Implementierung des Galileo-Systems im Weltraum auch die Maut mit Hilfe dieses Signals zu erheben.

11. Lassen das Mautgesetz bzw. die ausführenden Gesetze und Verordnungen nach Auffassung der Bundesregierung zu, dass per richterlichen Beschluss die Überwachung oder Herausgabe von Daten aus dem Mautsystem angeordnet werden können?

    Handelt es sich bei dem Mautsystem um ein Telekommunikationsmittel, dessen Überwachung nach der Strafprozessordnung nach entsprechendem richterlichen Beschluss zulässig ist?

Der Gesetzgeber hat eindeutige datenschutzrechtliche Regelungen in den §§ 4, 7 und 9 ABMG getroffen. Nach § 4 Abs. 2 Satz 3 und § 7 Abs. 2 Satz 2 ABMG dürfen die Mauterhebungs- und Mautkontrolldaten ausschließlich zum Zwecke des ABMG verarbeitet und genutzt werden.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333